BEST AVAILABLE COPY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-290389

(43)Date of publication of application : 04.10.2002

(51)Int.Cl. H04L 9/08
G06F 17/60

(21)Application number : 2001-084298

(22)Date of filing : 23.03.2001

(71)Applicant : HITACHI LTD

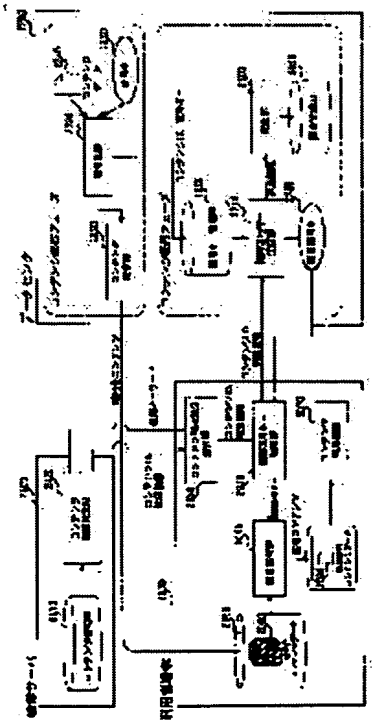
(72)Inventor : SHIRAISHI MASAHISA
IWASAKI KAZUMASA
KOBAYASHI RIE
KOIKE HIROSHI
HATOOKA JUNICHI

(54) DATA DECODING METHOD, DATA DECODER, AND DATA SALES SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data decoding method and device that decodes encrypted data only for a partial range of the data when the encrypted data are decoded and to provide a data sales system that decodes encrypted data having been given to a user in advance only for part of the data desirably used by the user and can impose the utility charge of the limited data part only onto the user.

SOLUTION: A decoding key used to decode data whose partial range is selected and utilized such as video, music or electronic book data includes a key to decode the entire data and partial range information for decoding. In the case of decoding the data, only the partial range data included in the decoding key are decoded and outputted. Furthermore, in a contents data sales system, only a specific range as above is decoded, a decoding key to decode only a required part of encrypted data by a user and distributed in advance to the user is produced, only the required part of the encrypted data is decoded by using the decoding key and the decoded data are provided to the user, and the decoding key is sold to impose the utility charge of the required part only



onto the user.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

拒絶引用S14 P0383W000

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－290389
（P2002－290389A）
(43)公開日　平成14年10月４日(2002.10.4)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ０６Ｆ　17/60	５１２	５Ｊ１０４
Ｇ０６Ｆ　17/60	５１２	Ｈ０４Ｌ　9/00	６０１Ｂ	

審査請求　未請求　請求項の数11　ＯＬ　（全 21 頁）

(21)出願番号　特願2001－84298(P2001－84298)

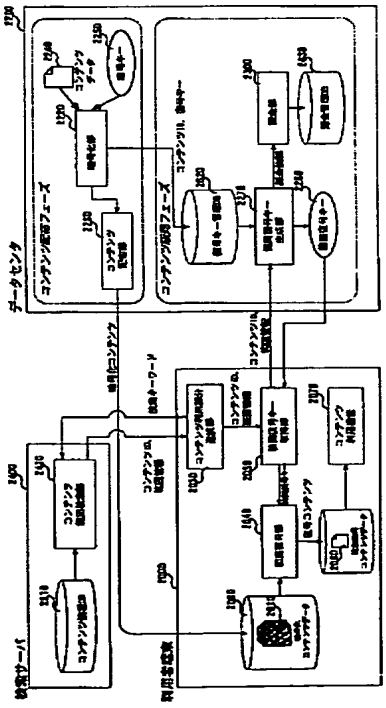
(22)出願日　平成13年３月23日(2001.3.23)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　白石　匡央
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスソリューション事業部内
(74)代理人　100096954
弁理士　矢島　保夫

最終頁に続く

(54)【発明の名称】　データ復号化方法、データ復号化装置、およびデータ販売システム

(57)【要約】
【課題】暗号化データの復号化においてデータの部分範囲に限って復号化を行うデータ復号方法及び装置を提供するとともに、あらかじめ利用者に渡された暗号化データに対し、そのデータの利用したい部分のみを復号化して利用させ、同時にその部分のみの利用料を課金することができるデータ販売システムを提供することことを目的とする。
【解決手段】映像や音楽、または電子書籍のデータのように、その部分範囲を選択して利用できるデータに対し、これを復号する復号キーの中にデータ全体を復号するキーと復号する部分範囲情報を含ませる。データ復号時には復号キーに含まれる部分範囲のみを復号化し出力する。また、コンテンツデータ販売システムにおいて、このような特定の範囲のみを復号化するようにし、利用者にあらかじめ配布された暗号化データに対して、利用者が必要とする部分のみを復号する復号キーを作成し、その復号キーにより暗号化データの中の利用部分のみを復号化して利用者に提供して、その復号キーを販売することにより利用部分のみの利用料を課金する。



【特許請求の範囲】
【請求項１】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、
暗号化されたデータはその暗号化の前または後のいずれかの状態において部分範囲を選択可能なデータであり、
選択された部分範囲の復号化データを取得するために与えられる範囲復号キーは、前記暗号化されたデータの全体または一部分を復号するための復号キーと復号範囲情報とを含み、前記暗号化されたデータに対して前記復号キーを用いて範囲復号処理を施すことにより、前記復号範囲情報で指定された部分範囲のみの復号化データを出力することを特徴とするデータ復号化方法。
【請求項２】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、
前記暗号化されたデータは、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであり、
前記暗号化されたデータ中の選択された部分範囲の復号化の処理は、
前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、
前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化するステップと、
復号化した前記部分範囲のデータを出力するステップとを備えていることを特徴とするデータ復号化方法。
【請求項３】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、
前記暗号化されたデータは、その全体が１つの復号キーで復号化できる１つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであり、
前記暗号化されたデータの選択された部分範囲の復号化の処理は、
前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、
前記暗号化されたデータ全体を、前記復号キーを用いて、復号化するステップと、
復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力するステップとを備えていることを特徴とするデータ復号化方法。
【請求項４】請求項１から３の何れか１つに記載のデータ復号化方法において、
前記復号キーには、復号キー発行元の電子署名を付加し、データの復号化時に該電子署名を検定することを特徴とするデータ復号化方法。
【請求項５】請求項１から４の何れか１つに記載のデータ復号化方法において、
前記復号キーは、復号キー発行元と復号化装置とが共有する秘密キーで暗号化してあることを特徴とするデータ復号化方法。
【請求項６】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化装置であって、
復号化の対象である前記暗号化されたデータは、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであり、
前記暗号化されたデータ中の選択された部分範囲の復号化を行うため、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力する手段と、
前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化する手段と、
復号化した前記部分範囲のデータを出力する手段とを備えたことを特徴とするデータ復号化装置。
【請求項７】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化装置であって、
復号化の対象である前記暗号化されたデータは、その全体が１つの復号キーで復号化できる１つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであり、
前記暗号化されたデータの選択された部分範囲の復号化を行うため、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力する手段と、
前記暗号化されたデータ全体を、前記復号キーを用いて、復号化する手段と、
復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力する手段とを備えたことを特徴とするデータ復号化装置。
【請求項８】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化プログラムであって、
それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであるような暗号化されたデータを復号化の対象とし、
前記暗号化されたデータ中の選択された部分範囲の復号化の処理として、
前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中

の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、
前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化するステップと、
復号化した前記部分範囲のデータを出力するステップとを備えていることを特徴とするデータ復号化プログラム。
【請求項９】暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化プログラムであって、
その全体が１つの復号キーで復号化できる１つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであるような暗号化されたデータを復号化の対象とし、
前記暗号化されたデータの選択された部分範囲の復号化の処理として、
前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、
前記暗号化されたデータ全体を、前記復号キーを用いて、復号化するステップと、
復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力するステップとを備えていることを特徴とするデータ復号化プログラム。
【請求項１０】コンテンツデータを管理するデータセンタと、ネットワーク経由で該データセンタに接続し前記コンテンツデータを購入する利用者端末とを備えたデータ販売システムであって、
前記利用者端末は、
利用者があらかじめ取得している暗号化データに対して、該データ中の利用部分の範囲を選択する手段と、
選択された利用部分の範囲を復号化するための範囲復号キーを前記データセンタに要求する手段と、
前記要求に応じて前記データセンタから送信される範囲復号キーを取得する手段と、
取得した範囲復号キーを用いて前記暗号化データの利用部分の範囲を復号化し、該利用部分の範囲の復号化データのみを出力する手段とを備え、
前記データセンタは、
前記利用者端末からの要求に応じて、前記利用部分の範囲を復号化するための範囲復号キーを生成して、前記利用者端末に送信する手段を備えたことを特徴とするデータ販売システム。
【請求項１１】請求項１０に記載のデータ販売システムにおいて、
前記データセンタは、前記範囲復号キーの生成に連携して、該利用部分の範囲に応じた課金を行う手段を、さらに備えたことを特徴とするデータ販売システム。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、暗号化データを復号化する技術に関し、特に、部分範囲を選択可能なデータを扱うデータ復号化方法および装置、並びに暗号化データを復号する復号キーを販売するデータ販売システムに関する。
【０００２】
【従来の技術】ネットワーク、特にインターネットを用いたオンライン販売システムにおいて、アプリケーションソフトウェアや、または書籍や映像、音楽などのデータをデジタル化したデータなどのいわゆるデジタルコンテンツの販売が行われている。これらの販売システムでは、ネットワークにより販売データの配送を行う「データのダウンロード販売」が行われている。
【０００３】デジタルコンテンツデータは簡単にコピーできてしまうため、コンテンツ販売システムにおいては、コンテンツの不正使用防止を目的としてコンテンツデータに対し暗号化処理を施すことが行われている。ここで、暗号化とはデータの使用にあたって復号手続きを必要とするようにデータの状態を変えることを示している。一般的な暗号化方法のＤＥＳ（Data Encryption Standard）やＲＳＡなどだけでなく、例えばデジタル映像データに対し可視透かしを入れたり、デジタル音楽データに対しある種のノイズを挿入するなど、データの品質を下げる加工を施し、そしてその状態を解除し品質の高いデータに復元することができるようなデータ変換処理もここでは暗号化方法とみなす。
【０００４】デジタルコンテンツのダウンロード販売において、映像や音楽などのデータサイズが大きいデジタルコンテンツを扱う場合にはそのダウンロード待ち時間が問題になる。この待ち時間を縮小するため、利用者に対しデジタルコンテンツデータをあらかじめ配布しておく方法がある。あらかじめ配布されるコンテンツデータは暗号化されており、利用者はデータの利用時に暗号を解除する復号キーを購入し、復号キーを用いて暗号を解除してコンテンツデータを利用する。例えば、シェアウェアのソフトウェアは機能制限版をＣＤ－ＲＯＭなどで配布し、利用者はソフトウェアの制限を解除するキーを購入し、機能制限を解除して使用することができる。
【０００５】あらかじめ配布した暗号化データに対し復号キーを販売するシステムでは、復号キーの漏洩や複製、または捏造などにより不正にデータを復号化し利用されてしまうことによって、データ利用料を正しく課金することができなくなる問題がある。このため、データに対する暗号化処理・復号化処理の方法には特に配慮がなされている。例えば、特開平１１－３９２６２号公報に示されるように、あらかじめ配布された暗号化データを復号化する際、利用者の端末側の端末情報を暗号化してデータを管理するデータセンタへ送付し、データセン

タでは暗号化された端末情報を復号化し、それを利用者端末で復号化できる形式で暗号化して利用者端末へ送り返す。利用者端末では送り返された暗号化情報を復号化し、それと最初に送った端末情報とを比較し、一致している場合のみあらかじめ配布されたデータの復号化を行う。この技術では、あらかじめ配布された暗号化データを復号化する際に、前に利用者端末とデータセンタの間で相互の認証を厳密に行うことができる。

【０００６】

【発明が解決しようとする課題】あらかじめ暗号化データを配布する前記従来の方法においては、次のような問題がある。

【０００７】デジタルコンテンツのデータとして映像や、音楽、書籍などのデータは、そのデータの任意の部分範囲を選択して利用したいことがある。例えば、映像・音楽データの場合、データの始めから３０秒間分だけのデータを利用することや、また書籍データの場合、本の中のある章だけ利用することなどである。暗号化コンテンツデータを配布し、それを復号化して利用させる前記のデータ販売方法において、販売対象のコンテンツとして上述の任意の部分範囲を選択できるコンテンツデータを扱うためには、暗号化データから任意の部分範囲のみを復号化する手段が必要となる。しかし、従来の暗号データの復号化方法では暗号化データを任意の部分範囲のみを復号化することはできず、データの全範囲を復号化してしまう問題がある。

【０００８】この復号化の問題により、前記のデータ販売方法において利用者が部分範囲を使用したいと申請した場合に、利用させたくない部分を含む全範囲のデータを復号化し利用可能とさせてしまう問題がある。この際の課金において、部分範囲の利用料のみを課金した場合には、販売者と利用者の間で申請範囲以外の部分の不正利用を行わないように信用取引的な面が生じてしまい、また全範囲分の利用料を課金する場合は、使用しない部分の料金を払わなければならなくなり、単価の高いデータなどでは利用者にとって負担が大きくなる問題がある。

【０００９】本発明は、上述の従来技術における問題点に鑑み、暗号化データの復号化においてデータの部分範囲に限って復号化を行うデータ復号方法及び装置を提供するとともに、あらかじめ利用者に渡された暗号化データに対し、そのデータの利用したい部分のみを復号化して利用させ、同時にその部分のみの利用料を課金することができるデータ販売システムを提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、暗号化されたデータはその暗号化の前または後のいずれかの状態において部分範囲を選択可能なデータであり、選択された部分範囲の復号化データを取得するために与えられる範囲復号キーは、前記暗号化されたデータの全体または一部分を復号するための復号キーと復号範囲情報とを含み、前記暗号化されたデータに対して前記復号キーを用いて範囲復号処理を施すことにより、前記復号範囲情報で指定された部分範囲のみの復号化データを出力することを特徴とする。

【００１１】また本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、前記暗号化されたデータは、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであり、前記暗号化されたデータ中の選択された部分範囲の復号化の処理は、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化するステップと、復号化した前記部分範囲のデータを出力するステップとを備えていることを特徴とする。

【００１２】また本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化方法であって、前記暗号化されたデータは、その全体が１つの復号キーで復号化できる１つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであり、前記暗号化されたデータの選択された部分範囲の復号化の処理は、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、前記暗号化されたデータ全体を、前記復号キーを用いて、復号化するステップと、復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力するステップとを備えていることを特徴とする。

【００１３】また本発明は、上述のデータ復号化方法において、前記復号キーには、復号キー発行元の電子署名を付加し、データの復号化時に該電子署名を検定することを特徴とする。

【００１４】また本発明は、上述のデータ復号化方法において、前記復号キーは、復号キー発行元と復号化装置とが共有する秘密キーで暗号化してあることを特徴とする。

【００１５】さらに本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化装置であって、復号化の対象である前記暗号化されたデータは、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号

化されたデータの部分範囲を選択可能なものであり、前記暗号化されたデータ中の選択された部分範囲の復号化を行うため、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力する手段と、前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化する手段と、復号化した前記部分範囲のデータを出力する手段とを備えたことを特徴とする。

【００１６】また本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化装置であって、復号化の対象である前記暗号化されたデータは、その全体が１つの復号キーで復号化できる１つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであり、前記暗号化されたデータの選択された部分範囲の復号化を行うため、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力する手段と、前記暗号化されたデータ全体を、前記復号キーを用いて、復号化する手段と、復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力する手段とを備えたことを特徴とする。

【００１７】さらに本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化プログラムであって、それぞれが同一のキーで復号化できる複数の暗号化データの集合であり、その部分集合によって前記暗号化されたデータの部分範囲を選択可能なものであるような暗号化されたデータを復号化の対象とし、前記暗号化されたデータ中の選択された部分範囲の復号化の処理として、前記暗号化されたデータを構成する各暗号化データの何れをも復号可能な復号キーと前記暗号化されたデータ中の復号すべき部分として選択された部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、前記暗号化されたデータ中の前記復号範囲情報で指定される部分範囲のみを、前記復号キーを用いて、復号化するステップと、復号化した前記部分範囲のデータを出力するステップとを備えていることを特徴とする。

【００１８】また本発明は、暗号化されたデータに対し復号キーを用いてデータを復号化するデータ復号化プログラムであって、その全体が１つの復号キーで復号化できる１つの暗号化データとして表現され、その暗号化前のデータは所定の部分範囲を選択できるデータであるような暗号化されたデータを復号化の対象とし、前記暗号化されたデータの選択された部分範囲の復号化の処理として、前記暗号化されたデータ全体を復号可能な復号キーと前記データ中の復号すべき部分範囲を指定する復号範囲情報とを含む範囲復号キーを入力するステップと、前記暗号化されたデータ全体を、前記復号キーを用いて、復号化するステップと、復号化したデータ中の前記復号範囲情報で指定された部分範囲のみを復号化データとして出力するステップとを備えていることを特徴とする。

【００１９】さらに本発明は、コンテンツデータを管理するデータセンタと、ネットワーク経由で該データセンタに接続し前記コンテンツデータを購入する利用者端末とを備えたデータ販売システムであって、前記利用者端末は、利用者があらかじめ取得している暗号化データに対して、該データ中の利用部分の範囲を選択する手段と、選択された利用部分の範囲を復号化するための範囲復号キーを前記データセンタに要求する手段と、前記要求に応じて前記データセンタから送信される範囲復号キーを取得する手段と、取得した範囲復号キーを用いて前記暗号化データの利用部分の範囲を復号化し、該利用部分の範囲の復号化データのみを出力する手段とを備え、前記データセンタは、前記利用者端末からの要求に応じて、前記利用部分の範囲を復号化するための範囲復号キーを生成して、前記利用者端末に送信する手段を備えたことを特徴とする。

【００２０】また本発明は、上述のデータ販売システムにおいて、前記データセンタは、前記範囲復号キーの生成に連携して、該利用部分の範囲に応じた課金を行う手段を、さらに備えたことを特徴とする。

【００２１】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【００２２】図１は、本発明の第１の実施形態のデータ復号化方法とそれに用いる暗号化データと復号キーの概念を示す。範囲復号装置１２２０は、暗号化データ１２００と範囲復号キー１２６０を入力とし、範囲復号キー１２６０の中の復号範囲１０３０で示される暗号化データ１２００の部分範囲のみを復号化して、復号化範囲データ１２５０を出力する。

【００２３】暗号化データ１２００は、その暗号化データ自身またはその暗号化前の元データが、論理的にまたは物理的にその部分範囲を選択できるデータである。例えば、データとして電子書籍データを考えた場合には、ページ番号を用いて電子書籍データの部分範囲を選択することができる。また、映像データを考えた場合には、映像の開始時間と終了時間を指定することで、映像データの部分範囲を選択することができる。さらに、前記のような時間やページ番号で順序付けられた連続データの部分範囲を選択することだけでなく、例えば同一内容を示す英語、日本語、ドイツ語、および中国語の文書を纏めて管理する複合文書データの中から日本語の文書だけを選択することもデータの部分範囲の選択である。また、写真集のデータのように、複数の写真データの集合データの中からキーワード「夕日」に合う写真データを

選択するようなことも、データの部分範囲の選択である。

【００２４】暗号化データ１２００は、ある部分単位の暗号化データ１２８０の集合として表されており、それぞれの部分単位の暗号化データ１２８０は全て同一キーで復号化できるように暗号化されている。例えば、暗号化データ１２００として、電子書籍のデータを考える場合、ページごとに同一キーで暗号化したページデータの集合として表すことができる。また、映像データを考える場合、個々のフレーム画像を同一キーで暗号化したフレーム画像データの集合として表すことができる。また、前記写真集の暗号化データも、個々の写真を同一キーで暗号化したデータの集合として表されている。つまり、ここでいう部分単位とは、電子書籍データの場合は各ページのデータに相当し、映像データの場合は各フレーム画像のデータに相当するものである。暗号化データ１２００は、写真集データのように部分単位暗号化データ１２８０の個々のファイルの集合と表されることもあれば、映像データのように１つの映像データファイル、例えばＭＰＥＧファイルのような形のこともある。映像ファイルの場合は、１つのファイルの中に複数のフレーム画像のデータを含んでおり、フレーム画像集合を纏めたファイルとみなすことができる。

【００２５】本実施形態のデータ復号化方法は、上述したような、あるデータの中からその部分データを選択できるようなデータを対象とするものである。

【００２６】図１において、範囲復号キー１２６０は、何れの部分単位の暗号化データをも復号できる全体復号キー１２７０と、データの中からその部分範囲を選択する復号範囲情報１０３０とを含んでいる。復号範囲情報１０３０は、例えば、暗号化データ１２００が電子書籍データの場合なら開始ページ番号と終了ページ番号であり、暗号化データ１２００が映像データなら開始時間と終了時間である。全体復号キー１２７０は、個々の暗号化部分データ１２８０を復号する共通の復号キーである。復号化範囲データ１２５０は、暗号化データ１２００の中の復号範囲情報１０３０で選択された部分範囲１２１０を復号化したデータである。

【００２７】範囲復号装置１２２０は、範囲選択部１２３０と復号化部１２４０を備える。範囲選択部１２３０は、部分単位暗号データ１２８０の集合である暗号化データ１２００の中から、範囲復号キー１２６０の中の復号範囲情報１０３０に従い、選択範囲データ１２１０を抜き出す。例えば、暗号化したページデータの集合として表される電子書籍のデータの場合には、開始ページ番号と終了ページ番号で構成される復号範囲情報１０３０で指定されたページのみを選択し出力する。また、個々のフレーム画像が暗号化された映像データの場合は、開始時間と終了時間で構成される復号範囲情報１０３０で指定された時間区間に含まれるフレーム画像を抜き出し出力する。復号化部１２４０は、選択範囲データ１２１０の個々のデータ１２９０に対し、範囲復号キー１２６０に含まれる全体復号キー１２７０を用いてデータの復号化を行い、復号化範囲データ１２５０を出力する。

【００２８】図１では、復号化範囲データ１２５０として復号化した部分単位データのみを出力しているが、これは暗号化データ１２００全体の中で復号範囲１２１０のみを復号化したデータ集合として出力しても良い。例えば、３０分の暗号化映像データに対し、復号範囲１０３０で示される区間が先頭から１０分を示していた場合、先頭から１０分のみの映像データを出力する形態もあれば、先頭から１０分のみが視聴できる状態になっている３０分の映像データとして出力する形態もある。

【００２９】暗号化データ１２００の中の部分集合１２１０のみを復号化する方法として、部分単位データをそれぞれ別々のキーで暗号化し、復号化時に復号範囲に対応する部分単位データの復号キーを全て渡すようにするような方法が考えられる。しかし、この方法では、範囲復号キー１２６０に全ての復号キーを含めなければならず、復号範囲の大きさに比例して長くなってしまう。また、全ての部分単位データに対する復号キーを管理しなければならない問題がある。例えば、映像のフレーム画像に対し前記方法を採るならば、映像１秒当たり３０枚のフレーム画像があるため、１時間の映像の場合では１０万個のキーを管理しなければならない。本実施形態によれば、１つの映像、すなわちフレーム画像の集合データに対し１つのキーを管理するだけでよく、範囲復号キーには１つの全体復号キーを含ませるだけで部分範囲の復号化を行うことができる。

【００３０】図２は、本実施形態のデータ復号化方法を用いたコンテンツデータ販売システムの構成を示す図である。以降では、このシステムにおけるデータ販売の処理手順を用いて本実施形態のデータ復号化方法を説明する。本実施形態のコンテンツ販売システムは、ネットワーク２５００に接続された、利用者端末２０００、データセンタ２２００、及び検索サーバ２４００を備える。利用者端末２０００はネットワーク２５００を介してコンテンツを購入し、利用するための装置である。データセンタ２２００は、コンテンツを利用する利用者に対しコンテンツデータの配布とコンテンツデータの利用による課金を行う。検索サーバ２４００は、利用者がコンテンツデータ購入のために欲しいコンテンツを検索したいとき、利用者に検索機能を提供する装置である。

【００３１】利用者端末２０００は、コンテンツデータの復号処理や利用などのためのプログラムを格納する二次記憶装置２０１０、暗号化コンテンツデータを格納する二次記憶装置２０８０、メモリ２１００、ＣＰＵ２１１０、及びネットワークインタフェース２１２０を備えており、これら各部はバス２１３０で接続されている。

【００３２】二次記憶装置２０８０に格納される暗号化

コンテンツデータ２０９０は、あらかじめ利用者に配布されたデータである。一般的なデータダウンロード販売の方式として、利用者のデータ利用時に、オンデマンドにデータセンタからコンテンツデータをダウンロードする方式がある。これに対し、本実施形態の方式では、事前に利用者に対しコンテンツデータを配布している。これにより、利用者のデータ利用時のデータダウンロード待ち時間を減らすことができる。

【００３３】コンテンツデータの事前配布方法は、例えばＣＤ－ＲＯＭ、あるいはＤＶＤ－ＲＯＭなどの大容量メディアにコンテンツデータを格納し、それらを陸送などで配布すればよい。ある程度の量のコンテンツデータを纏めて配布することにより、ネットワーク転送よりも陸送の方がデータ転送のコストを安く抑えることができる。また別のデータ配布方法として、利用者がネットワークを使用していない時間等に、利用者の利用要求とは非同期にデータの転送を行う方法もある。

【００３４】どのコンテンツデータを配布するかに対しては、データセンタが管理する全てのコンテンツデータを配布する方法が考えられる。このようにすれば、コンテンツデータのダウンロード時間は０にできる。しかし、実際には全てのデータを送付することはデータ量から考えると難しく、事前配布するデータは配布可能な量だけを選択して配布することになる。この場合、事前配布されたデータはキャッシュ的に使われるようになる。すなわち、利用者の希望するデータが、既に配布されている場合はそれを用い、配布されていない場合はデータセンタ２２００からダウンロードする。利用者に対し事前に配布するコンテンツデータの決め方は、過去のデータ利用統計により人気の高いデータを送付したり、利用者に対し事前にアンケートをとり、その結果から興味がありそうなデータを送付するなどの方法がある。

【００３５】データ配布方法の別の形態として、広帯域ネットワークでデータセンタと接続されたコンテンツデータの販売端末から、ある程度纏まった量のデータを一括でダウンロードしておく方法などもある。この場合に、例えば電子書籍のデータに対して、ある本の一部だけを使用したいという利用者の要求に対し、販売端末からは本全体のデータをダウンロードさせて、その中の利用したい部分だけを使用させることができる。利用者がその本の別の部分を利用したいときには、その本の当該範囲を復号化する復号キーを購入することにより利用できる。これにより、データのダウンロード時間が必要なくなる。

【００３６】これら事前に配布するコンテンツデータは、利用者による料金の支払いより前にデータが渡される。そのため、利用者に料金を払っていないコンテンツデータを利用させないように、データに暗号化を施しておく必要がある。

【００３７】二次記憶装置２０１０には、オペレーティングシステム（以下、ＯＳと記述する）２０２０、利用者が暗号化コンテンツデータ２０９０の利用する部分を選択するためのコンテンツ利用部分選択部２０３０、データセンタ２２００にコンテンツ利用部分を復号するためのキーを要求する範囲復号キー取得部２０５０、範囲復号キーを用いて暗号化コンテンツデータ２０９０を復号し、その部分範囲を出力する範囲復号部２０４０、範囲復号部２０４０により出力された範囲復号コンテンツデータ２０６０、およびその部分範囲の復号されたコンテンツデータ２０６０を利用するコンテンツ利用機能２０７０が格納される。

【００３８】コンテンツ利用部分選択部２０３０は、例えば、対象とするデータが電子書籍のデータである場合には利用者に読みたいページ番号を選択させ、また対象データが映像データである場合は利用者に視聴したい時間区間を選択させるような、コンテンツデータの中から利用したい部分を選択させる手段を提供する。このコンテンツデータの部分範囲の選択方法として、検索サーバ２４００を用いて、利用者が入力した検索キーワードによりＤＢ検索を行い、検索キーワードに該当するコンテンツデータの範囲を取得する方法がある。すなわち、データ販売システムとして、利用者がＤＢ検索を行い、その結果に該当するコンテンツデータを購入するシステム形態である。

【００３９】また、別の実施形態のシステムとして、利用者に配布した暗号化コンテンツデータ２０９０を利用者が試写・試聴して、利用する範囲を選択するシステムも考えられる。例えば、扱うコンテンツデータが映像データの場合において、利用者が映像データを編集して番組制作などに利用する目的で使用する場合を考える。このとき、あらかじめ配布する暗号化コンテンツデータ２０９０に対し、各フレーム画像に可視透かしを挿入して配布する。こうすることにより、配布映像データは試写・仮編集用途では用いることができるが、番組制作などの本編集用途では使用できないようになっている。利用者は、可視透かしの入った映像をコンテンツ利用部分選択手段２０３０で試写しながら映像の利用部分を決定し、その部分の可視透かしを取り去る範囲復号キーの取得要求を出す。そして復号キー取得し、その復号キーを用い利用部分の可視透かしを取り除いて本編集用途で使用する。

【００４０】コンテンツ利用機能２０７０は、電子書籍データのページを表示するビューア、または映像データを再生するプレイヤなどと同等のものであり、コンテンツデータを利用者に利用させる機能を有する。

【００４１】データセンタ２２００は、コンテンツデータの管理や利用者の管理などを行うためのプログラムを格納する二次記憶装置２２１０、メモリ２３２０、ＣＰＵ２３３０、およびネットワークインタフェース２３４０を備え、これら各部はバス２３５０で接続されてい

る。

【００４２】二次記憶装置２２１０には、ＯＳ２２６０、販売するためのコンテンツデータ２２４０、それを利用者へ配布する際に暗号化する暗号化部２２２０、その暗号キー２２５０、暗号化したコンテンツを利用者へ配布するコンテンツ配布部２２３０、利用者に配布したコンテンツデータとそれに対応する復号キーを管理する復号キー管理テーブル２２９０、利用者から要求されたコンテンツデータの部分範囲を復号するキーを作成する範囲復号キー生成部２２７０、それにより生成された範囲復号キー２２８０、復号キー生成に連携して課金を行う課金部２３００、および利用者に対する課金の状況を管理する課金管理テーブル２３１０が格納される。

【００４３】検索サーバ２４００は、コンテンツデータの範囲情報などを格納する二次記憶装置２４１０、メモリ２４５０、ＣＰＵ２４６０、およびネットワークインタフェース２４７０を備え、これら各部はバス２４８０で接続されている。

【００４４】二次記憶装置２４１０には、ＯＳ２４４０、コンテンツデータの範囲を管理するコンテンツ情報テーブル２４３０、コンテンツ情報テーブル２４３０を用いてコンテンツの範囲検索を行うコンテンツ範囲検索部２４２０が格納される。

【００４５】以降では、図２に示すコンテンツデータ販売システムにおいて、扱うコンテンツデータが映像データの場合について、本発明の実施形態を説明する。

【００４６】図３は、図２で示されるコンテンツデータ販売システムにおける各機能モジュールの関連とデータの流れを示している。図３を用いて、コンテンツデータの部分範囲の販売方法について説明する。

【００４７】コンテンツデータ販売システムの全体処理の流れは次の通りである。本実施形態におけるコンテンツデータの販売システムでは、利用者はコンテンツデータを提供・管理するデータセンタ２２００と契約する。そして、データセンタ２２００は、契約した利用者に対し、あらかじめ暗号化されたコンテンツデータを配布する。利用者は、検索サーバ２４００を用いて利用したいコンテンツデータをキーワード検索する。利用者は、検索結果に対応する暗号化コンテンツデータを復号する復号キーをデータセンタから購入する。そして、配布されている暗号化コンテンツデータの中の利用したいコンテンツデータに対し、復号キーを用いてデータを復号化し利用する。

【００４８】コンテンツデータの配布に際しては、まずデータセンタ２２００において、暗号化部２２２０により、暗号キー２２５０を使い配布対象のコンテンツデータ２２４０を暗号化する。暗号化部２２２０は、暗号化したコンテンツデータの識別子であるコンテンツＩＤとそのコンテンツを復号するための復号キーを復号キー管理ＤＢ２６２０へ格納する。この情報は、配布した暗号化コンテンツを復号する範囲復号キー作成時に用いられる。暗号化したコンテンツは、コンテンツ配布部２２３０によって利用者端末２０００に配布される。配布された暗号化コンテンツ２０９０は、利用者端末２０００に接続されている二次記憶装置２０８０に格納される。コンテンツ配布部２２３０による配布の方法は、上述した通り、データを大容量メディアに格納して陸送する方法や、コンテンツ販売端末により利用者にダウンロードさせる方法などがある。

【００４９】利用者は、コンテンツ利用部分選択部２０３０を用い、希望するコンテンツデータの検索を行う。コンテンツ利用部分選択部２０３０は、検索サーバ２４００のコンテンツ範囲検索部２４２０へ、利用者より入力されたコンテンツデータ検索キーワードを渡し、コンテンツデータの検索を依頼する。コンテンツ範囲検索部２４２０は、コンテンツ情報ＤＢ２６１０のデータを用い、検索キーワードに合うコンテンツデータのコンテンツＩＤとその範囲情報を取得する。これにより、利用者は利用を希望するコンテンツデータの情報を取得する。

【００５０】次に、利用者は、利用したいコンテンツデータに対し、そのデータを復号する復号キーを購入する。範囲復号キー取得部２０５０は、コンテンツ利用部分選択部２０３０により選択されたコンテンツデータのコンテンツＩＤとその範囲情報を用い、データセンタ２２００にそのコンテンツの部分範囲を復号する範囲復号キーの作成を依頼する。データセンタ２２００の範囲復号キー生成部２２７０は、そのコンテンツＩＤに対する全体復号キーを復号キー管理ＤＢ２６２０から取得し、これと範囲情報を組み合わせて範囲復号キー２２８０を作成する。この際、課金部２３００を用いて範囲復号キーに対する課金処理を行う。これにより、利用者に対して範囲復号キーを渡し暗号化コンテンツの部分範囲を利用させることができ、さらにデータセンタ側でコンテンツデータの部分範囲の利用料を徴収することができる。

【００５１】利用者は、範囲復号キー取得部２０５０により取得した範囲復号キーにより範囲復号部２０４０を用い、部分範囲のみ復号化した範囲復号コンテンツデータ２０６０を取得する。コンテンツ利用機能２０７０を使って、取得した範囲復号コンテンツデータを利用する。

【００５２】以上の処理により、利用者にあらかじめ配布された暗号化データに対して、利用者が必要とする部分のみを利用させることができ、またその利用部分に応じた利用料を課金することができる。

【００５３】図４は、映像データの場合におけるデータの暗号化と部分範囲の復号化の方式を示す概念図である。図４を用いて、映像データにおけるデータ暗号化・復号化方式を説明する。元映像データ３０００は、販売対象となるデータであり、図３のコンテンツデータ２２４０に相当する。映像データ３０００は、フレーム画像

３０１０～３０７０の集合データと見なすことができる。図３の暗号化部２２２０は、各フレーム画像３０１０～３０７０に対し同一キーで暗号化を施し、暗号化フレーム画像３１１０～３１７０を作成する。これら暗号化フレーム画像３１１０～３１７０を組み合わせ、暗号化映像データ３２００を作成する。この暗号化映像データ３２００を利用者へ配布する。これは、図３の暗号化コンテンツデータ２０９０に相当する。

【００５４】コンテンツ利用部分選択部２０３０により、時間の形式で示される映像データの範囲３２１０が選択され、この範囲を復号する範囲復号キーが生成されることになる。範囲復号部２０４０は、範囲復号キーを用いその中に含まれる範囲情報３２１０に従い、その範囲に含まれるフレーム画像３２２０～３２４０を抜き出す。そして、フレーム画像３２２０～３２４０を復号化して、復号化フレーム画像３２５０～３２７０を作成する。このフレーム画像３２５０～３２７０を組み合わせ、範囲復号映像データ３３００を作成する。

【００５５】図５に、復号キー管理テーブル２２９０の例を示す。ここでは、コンテンツデータが映像データの場合を例として示す。復号キー管理テーブル３５００は、映像データを識別する値であるコンテンツＩＤ３５１０と、そのデータを復号する復号キー３５２０と、そのデータの全範囲の大きさを示す先頭時間３５３０と、終了時間３５４０とから構成される。例えば、レコード３５５０は、「ＨＩ０００８１１０１．ｍｐｇ」という映像ファイルに対し、その復号化キーは「９８２Ｅ８ＢＤ」であることを示し、またそのデータは、先頭が「００：００：００：００」から始まり「０１：２０：００：００」で終了する１時間２０分の長さの映像データであることを示している。ここで、映像の時間を示す値「ａａ：ｂｂ：ｃｃ：ｄｄ」は、ａａ時間ｂｂ分ｃｃ秒のｄｄフレーム目を示し、映像の位置をフレーム単位で特定することができる表記法である。

【００５６】コンテンツデータの暗号方式は、復号キーを用いて復号可能な方式であれば、本発明に適用可能である。本実施形態では、７桁の１６進数値で復号できる暗号を用いている。

【００５７】復号キー管理テーブル２２９０には、データセンタ２２００において利用者へコンテンツデータを配布するためにデータの暗号化を行った際に、暗号化したデータのデータ名とそのデータの復号キーとデータの範囲とを追加する。復号キーは、利用者に配布するコンテンツデータごとに変更し、配布したデータとその暗号を復号するキーの対応を復号キー管理テーブル２２９０で管理している。コンテンツデータごとにキーを変更することにより、あるコンテンツデータに対する復号キーが漏洩しても、他のコンテンツデータの安全性は保つことができる。

【００５８】図５に示すように、復号キー管理テーブル３５００に、コンテンツデータ範囲の大きさ情報３５３０，３５４０を含むことにより、利用者からのコンテンツデータの部分範囲復号要求時に、その要求範囲が元のコンテンツデータの範囲に含まれているかの妥当性をチェックすることができる。

【００５９】図６に、範囲復号キー２２８０のデータ構造を示す。範囲復号キー２２８０は、コンテンツデータを識別するコンテンツＩＤ３６２０、そのコンテンツデータを復号する復号キー３６３０、およびコンテンツデータの部分範囲を示す値とで構成される。本実施形態では、映像データを扱うため、コンテンツデータの部分範囲を示す値は、開始時間３６４０、終了時間３６５０で構成される。

【００６０】図６の例では、「ＨＩ０００８１１０１．ｍｐｇ」という映像ファイルに対し、それを復号化するキーは「９８２Ｅ８ＢＤ」であり、そしてその映像ファイルを復号化する範囲は開始時間「００：２０：３０：１５」から終了時間「００：２２：１０：０７」までの区間であることを示している。

【００６１】図７に、コンテンツ情報テーブル２４３０の例を示す。コンテンツ情報テーブル２４３０は、利用者が利用したいコンテンツを検索するためのコンテンツ内容のキーワードを格納した映像内容情報３７００、コンテンツ内容キーワードに対応するコンテンツを識別するコンテンツＩＤ３７１０、およびキーワードに対応するコンテンツデータの範囲情報から構成される。本実施形態では、映像データを扱うため、コンテンツデータの範囲情報は、開始時間３７２０と終了時間３７３０で構成される。例えば、レコード３７４０では、映像内容のキーワードとして「春」、「青空」、「桜の花」、「名古屋城」に対応する映像データは、ファイル名「ＨＩ００８１１０１．ｍｐｇ」の開始時間「００：２０：３０：１５」から終了時間「００：２２：１０：０７」の部分であることを示している。

【００６２】図８に、課金管理テーブル２３１０の例を示す。課金管理テーブル２３１０は、課金に対する契約を識別する契約ＩＤ３８００、課金対象の利用者を識別する利用者ＩＤ３８１０、および課金の料金３８２０で構成される。課金は、範囲復号キーを発行する度に行う。範囲復号キー発行により、利用者に対し利用したい範囲のみを復号化し提供しているので、その範囲のみの利用料を課金することができる。

【００６３】次に図９から図１１のフローチャートに基づいて、本実施形態のシステムにおけるコンテンツデータ復号化の処理の流れを説明する。

【００６４】図９は、範囲復号キー取得部２０５０の処理手順を示すフローチャートである。

【００６５】まず、コンテンツ利用部分選択部２０３０から復号するコンテンツデータのコンテンツデータＩＤと範囲を受け取る（ステップ４０１０）。本ステップよ

り前に、コンテンツ利用部分選択部２０３０とそれに関連する機能ブロックにより次のような処理が行われているものとする。コンテンツ利用部分選択部２０３０は、利用者がコンテンツデータの利用したいデータ名とその範囲とを決定する手段を提供するもので、前述のように種々の方法を用いてよい。本実施形態では、検索サーバ２４００のコンテンツ検索部２４２０を用いてデータ名と範囲を取得する。例えば、利用者が「名古屋城」の映像が欲しいと思った場合、利用者は、コンテンツ利用部分選択部２０３０に検索キーワード「名古屋城」を渡す。コンテンツ利用部分選択部２０３０は、コンテンツ範囲検索部２４２０にキーワード「名古屋城」を渡しコンテンツデータの検索を依頼する。コンテンツ範囲検索部２４２０は、コンテンツ情報テーブル２４３０を用い、キーワード「名古屋城」が映像内容情報３７００に一致するレコード３７４０を取得し、そのコンテンツＩＤ「ＨＩ００００８１１０１．ｍｐｇ」と開始時間「００：２０：３０：１５」と終了時間「００：２２：１０：０７」をコンテンツ利用部分選択部２０３０に返す。コンテンツ利用部分選択部２０３０は、そのデータ名と範囲情報を範囲復号キー取得部２０５０に渡す。

【００６６】次に、受け取ったコンテンツデータＩＤと範囲を、範囲復号キー生成部２２７０に渡して範囲復号キーの生成を依頼し、その結果として範囲復号キーを取得する（ステップ４０２０）。

【００６７】さらに、範囲復号キーを範囲復号部２０４０に渡し、コンテンツデータ範囲復号要求を出す（ステップ４０３０）。この範囲復号キーの生成処理とコンテンツデータの範囲復号処理を、以下に説明する。

【００６８】図１０を用いて、範囲復号キーの生成手順を説明する。図１０は、範囲復号キー生成部２２７０の処理手順を示すフローチャートである。

【００６９】まず、範囲復号キー取得部２０５０からコンテンツＩＤと範囲を受け取る（ステップ４１１０）。このコンテンツＩＤを用いて、復号キー管理テーブル３５００からそのコンテンツＩＤに対応するデータの復号キーとそのデータの全体の範囲を取得する（ステップ４１２０）。例えば具体的には、復号キー管理テーブル３５００のコンテンツＩＤ「ＨＩ００００８１１０１．ｍｐｇ」に対応するレコード３５５０を取得し、その復号キー３５２０「９８２Ｅ８ＢＤ」、データ全体範囲として先頭時間３５３０「００：００：００：００」、終了時間３５４０「０１：２２：００：００」を取得する。

【００７０】次に、範囲復号キー取得部２０５０から受け取った範囲が、復号キー管理テーブル３５００から取得した全体範囲３５３０，３５４０の中に入っているかを調べる（ステップ４１３０）。例えば具体的には、部分範囲として開始時間「００：２０：３０：１５」から終了時間「００：２２：１０：０７」の範囲は、映像データ「ＨＩ００００８１１０１．ｍｐｇ」の全体範囲「００：００：００：００」～「０１：２０：００：００」の中に含まれているので、要求された範囲は正しいと認める。

【００７１】コンテンツＩＤ、復号キー、および範囲を組み合わせ、範囲復号キー本体を作成する（ステップ４１４０）。例えば具体的には、コンテンツＩＤ「ＨＩ００００８１１０１．ｍｐｇ」、開始時間「００：２０：３０：１５」、終了時間「００：２２：１０：０７」に対して、全体復号キー「９８２Ｅ８ＢＤ」を付加して、図６の範囲復号キー本体３６００のデータを作成する。

【００７２】範囲復号キー２２８０の発行に連携して課金処理を行う（ステップ４１５０）。課金処理は、課金部２３００に依頼して行う。課金処理において課金対象となる利用者が判別できるように、利用者がデータを利用する前にログインするシステム構成にしておく。または、範囲復号キー取得部２０５０が範囲復号キー生成を依頼する際に利用者ＩＤも送付するなどの仕組みにしておく。

【００７３】作成した範囲復号キー２２８０を範囲復号キー取得部２０５０へ渡し（ステップ４１６０）、処理を終了する。

【００７４】図１１を用いて、コンテンツデータの範囲復号処理を説明する。図１１は、範囲復号部２０４０の処理手順を示すフローチャートである。

【００７５】まず、コンテンツＩＤに対応する暗号化コンテンツデータ２０９０を取得する（ステップ４２２０）。コンテンツデータは二次記憶装置２０８０に格納されており、ここではＤＶＤ－ＲＯＭなどの大容量メディア、または販売端末でダウンロードするための読み書き可能なリムーバブルメディアを想定している。従って、必要に応じてメディアの交換を行う。すなわち、コンテンツＩＤに対応するコンテンツデータ２０９０を格納するメディアをドライブに挿入し読み出し準備を行ったのち、必要な暗号化コンテンツデータ２０９０を取得する。

【００７６】続いて、暗号化コンテンツデータ２０９０から部分データを取り出す。具体的には、図４に示すような暗号化映像データ３２００から、部分データとして個々のフレーム画像３１１０～３１７０を一つずつ取り出す（ステップ４２３０）。一つずつ順番に取り出したフレーム画像に対し、範囲復号キー２２８０の範囲情報３６４０，３６５０の範囲に含まれるかをチェックする。具体的には、図６に示す範囲復号キーの例の場合には、取り出したフレーム画像が「００：２０：３０：１５」から「００：２２：１０：０７」に含まれているかを調べる（ステップ４２４０）。範囲３６４０，３６５０に含まれるフレーム画像は、範囲復号キー２２８０の中の全体復号キー３６３０を用いて復号化する（ステップ４２５０）。範囲３６４０，３６５０に含まれないフレーム画像は破棄する（ステップ４２６０）。かかる処

理（ステップ４２３０～４２５０）を映像データを構成する全てのフレーム画像について繰り返す（ステップ４２７０）。

【００７７】ステップ４２５０で復号化された部分データを組み直し、範囲復号化コンテンツデータ２０６０を作成し出力する。具体的には、図４に示すように復号化されたフレーム画像３２５０，３２６０，３２７０を用い、このフレーム画像で構成される映像データ３３００を作成し（ステップ４２８０）、処理を終了する。

【００７８】以上の処理により、暗号化コンテンツデータ２０９０と範囲復号キー２２８０から部分範囲のみを復号化したデータを出力することができる。

【００７９】次に、図１２および図１３を参照して、本発明のデータ暗号化・復号化方式の第２の実施の形態を説明する。なお、第２の実施の形態において、第１の実施の形態と同様の部分は説明を省略する。

【００８０】図１２は、第２の実施の形態の範囲復号方式の概念図である。この範囲復号方式は、第１の実施の形態の暗号化データ１２００とは異なる形式のデータに対する範囲復号方式である。暗号化データ１０００は、データ全体が暗号化されているデータである。また、暗号化データ１０００は、その暗号化前のデータが任意の部分範囲を切り出すことができるデータである。第１の実施形態の暗号化データ１２００は部分単位暗号データ１２８０の集合として表されるのに対し、第２の実施形態の暗号化データ１０００は暗号化データの集合ではなく１つの暗号化データとして表現される。例えば、映像データを例に説明すると、第１の実施の形態では、映像データはフレーム画像の集合であり、各フレーム画像を暗号化した映像データとして扱っていた。第２の実施の形態では、映像データそのものを暗号化してしまい全体を１つの暗号データとして扱う方式を想定している。具体的には、映像データがＭＰＥＧファイルで表現されているときには、暗号化データ１０００はＭＰＥＧファイル自体を暗号化したデータになる。

【００８１】範囲復号装置１０４０は、図１と同様に暗号化データと範囲復号キー１０１０を受け取り、暗号化データの部分範囲１０９０を出力する。このとき用いる範囲復号キー１０１０は、第１の実施の形態と同様に、全体復号キー１０２０と復号範囲１０３０からなる。全体復号キー１０２０は、第１の実施の形態では暗号化データの個々の部分単位１２８０を復号化するキーであったのに対し、ここでは暗号化データ１０００を復号化するキーである。復号範囲１０３０は、第１の実施の形態と同様の値をとる。例えば、電子書籍のデータの場合はページ番号であり、映像データの場合は時間である。復号範囲１０３０は、暗号化データ１０００の部分範囲１１００を示している。

【００８２】範囲復号装置１０４０は、全体復号化部１０５０と範囲選択部１０８０を備える。全体復号化部１０５０は、範囲復号キー１０１０の中の全体復号キー１０２０を用いて暗号化データ１０００の復号化処理を行い、復号化データ１０６０を出力する。範囲復号キー１０１０の中の復号範囲情報１０３０は、復号化データ１０６０の中の部分範囲１０７０を示している。範囲選択部１０８０は、復号化データ１０６０から復号範囲情報１０３０で示される部分範囲を切り出し、復号化範囲データ１０９０を出力する。

【００８３】図１２では、復号化範囲データ１０９０として復号化したデータの部分範囲を切り出して出力しているが、これは暗号化データ全体の中で選択された部分範囲のみを復号化したデータでも良い。これは、暗号化データと出力される復号化データのデータの大きさは同じであり、復号キーで選択された部分のみ復号化されており、他の部分は暗号がかかったままのデータである。

【００８４】図１３を用いて、データ全体が暗号化されているデータに対する部分範囲復号化の処理を説明する。以下では、第２の実施の形態のデータ復号化方法を図２で示されるデータ販売システムに適用した場合を想定して、データ復号化方法の実施の形態を説明する。つまりは、図２の利用者端末２０００にあらかじめ配布した暗号化コンテンツデータ２０９０がデータ全体が暗号化された暗号化データ１０００であり、範囲復号部２０４０は暗号化データ１０００を復号化するものである。図１３は、この場合の範囲復号部２０４０の処理手順を示すフローチャートである。

【００８５】まず、範囲復号キーに含まれるコンテンツＩＤに対する暗号化コンテンツデータ２０９０を取得する（ステップ４３２０）。これは、第１の実施の形態で説明した図１１に示すフローチャートのステップ４２２０と同一の処理である。次に、暗号化コンテンツデータ２０９０を範囲復号キー１０１０の中の全体復号キー１０２０を用いてコンテンツデータ全体を復号化する（ステップ４３３０）。

【００８６】復号化コンテンツデータから部分データを一つずつ取り出し（ステップ４３４０）、その部分データが範囲復号キー２２８０の中の範囲３６４０，３６５０に含まれているかを調べる（ステップ４３５０）。具体的には、第１の実施の形態における図１１と同様に、映像データのフレーム画像を取り出し、そのフレーム画像が当該範囲に含まれているかを調べる。ここでは、第１の実施の形態における図１１の方式とは違い、フレーム画像は既に復号化されている。選択範囲に含まれる部分データは出力し（ステップ４３６０）、選択範囲に含まれない部分データは破棄する（ステップ４３７０）。コンテンツデータに含まれる全ての部分データに対し前記の範囲チェックを行う（ステップ４３８０）。

【００８７】以上の処理により、全体を暗号化したコンテンツデータに対しても、範囲復号キー２２８０を用いて部分範囲のみを復号化したデータを出力することがで

きる。

【００８８】次に、図１４～図１７を参照して、本発明のデータ暗号化・復号化方式の第３の実施の形態を説明する。なお、第３の実施の形態において、第１の実施の形態と同様の部分は説明を省略する。

【００８９】図１４は、第３の実施の形態の範囲復号方式の概念図である。第３の実施形態の暗号化データの範囲復号方式は、サイン（署名）データ５０１０を付加した範囲復号キー５０００を用いるものである。サインデータ５０１０は、全体復号キー１２７０と復号範囲１０３０の内容が正しいことを証明するためのデータであり、このサインデータ５０１０を検定することで範囲復号キーの改竄をチェックすることができる。これにより、あらかじめ配布された暗号化データ１２００を範囲復号キーを捏造することによって不正に利用されることを防ぐことができる。サインデータの検定については下記に述べる。ここで、暗号化データ１２００は第１の実施の形態と同様に部分単位暗号化データ１２８０の集合として表されるデータである。

【００９０】範囲復号化装置５０３０は、サイン検定部５０２０と、範囲取得部１２３０と、復号化部１２４０を備える。範囲復号化装置５０３０は、第１の実施の形態と同様に、暗号化データ１２００と範囲復号キー５０００を入力とし、復号化範囲データ１２５０を出力する。暗号化データ１２００と範囲復号キー５０００が入力されると、まず範囲復号キー５０００の中のサインデータ５０１０を、サイン検定部５０２０により検定し、範囲復号キー５０００の正当性をチェックする。ここで範囲復号キー５０００が正しくないと認められたら、範囲復号処理を中断し、復号化範囲データ１２５０を出力しない。これにより、不正な範囲復号キーの使用を防ぐことができる。サイン検定が行われた後、範囲取得部１２３０は、暗号化データ１２００の中から選択範囲データ１２１０を抜き出し、復号化部１２４０は、選択範囲データ１２１０を復号化して復号化範囲データ１２５０を出力する。この処理は、第１の実施の形態で示した範囲取得部１２３０および復号化部１２４０の処理と同様である。

【００９１】以下では、第３の実施の形態のデータ復号化方法を図２で示されるデータ販売システムに適用した場合を想定して、サイン付き範囲復号キー５０００を用いるデータ復号化方法の実施の形態を説明する。つまりは、図２のデータセンタ２２００の範囲復号キー生成部２２７０と利用者端末２０００の範囲復号部２０４０が、サイン付き範囲復号キー５０００を扱うよう処理が変更されているシステムである。

【００９２】図１５は、範囲復号キー５０００のデータ構造を示す。範囲復号キー５０００は、範囲復号キーの本体を格納する本体部分３６００と、そのデータに対する発行元のデータセンタ２２００のサイン（署名）を格納するサイン部分３６１０で構成される。

【００９３】データセンタのサイン３６６０を付加することにより、この範囲復号キー５０００を受け取る範囲復号部２０４０は、範囲復号キー本体３６００の改竄をチェックすることができる。すなわち、データセンタのサイン３６６０は、範囲復号キー本体３６００をデータセンタ２２００の秘密キーで暗号化したデータである。範囲復号部２０４０は、サイン３６６０をデータセンタ２２００の公開キーで復号化し、その復号化したデータと範囲復号キー本体３６００とが一致することを調べ、一致した場合には範囲復号キー本体３６００は正しいデータであると認める。

【００９４】範囲復号キー本体３６００は、図６と同様に、コンテンツデータを識別するコンテンツＩＤ３６２０、そのコンテンツデータを復号する復号キー３６３０、およびコンテンツデータの範囲を示す値で構成される。本実施の形態では映像データを想定しているため、コンテンツデータの範囲を示す値は開始時間３６４０と終了時間３６５０で構成される。

【００９５】図１６を用いて、サイン付き範囲復号キー５０００の作成処理を説明する。サイン付き範囲復号キー５０００の作成手順は、第１の実施の形態における図１０の範囲復号キー２２８０の作成手順とほぼ同じである。まず、範囲復号キー取得部２０５０からコンテンツＩＤと範囲を受け取る（ステップ４４１０）。このコンテンツＩＤを用いて復号キー管理テーブル３５００から当該コンテンツＩＤに対応するデータの全体復号キーとそのデータの全体の範囲を取得する（ステップ４４２０）。範囲復号キー取得部２０５０から受け取った範囲が、復号キー管理テーブル３５００から取得した全体範囲３５３０，３５４０の中に含まれているかを調べる（ステップ４４３０）。コンテンツＩＤ、復号キー、および範囲を組み合わせ、範囲復号キー本体３６００を作成する（ステップ４４４０）。ここまでは、第１の実施の形態の図１０に示すステップ４１１０～ステップ４１４０と同様である。

【００９６】次に、前ステップまでに作成された範囲復号キー本体３６００に対し、データセンタ２２００の秘密キーでサインする（ステップ４４５０）。具体的には、範囲復号キー本体３６００に対し、図１５に示すように、サインデータ３６６０が付加されることになる。つづいて、サイン付き範囲復号キー５０００の発行に連携して課金処理を行い（ステップ４４６０）、作成したサイン付き範囲復号キー２２８０を範囲復号キー取得部２０５０へ渡す（ステップ４４７０）。このステップは、第１の実施の形態における図１０のステップ４１５０およびステップ４１６０と同様である。

【００９７】図１７を用いて、サイン付き範囲復号キー５０００を用いて暗号化データの部分範囲を復号する処理を説明する。

【００９８】まず、範囲復号キー取得部２０５０から範囲復号キーを受け取り、サインの検定を行う。サインの検定により、範囲復号キーが正しくないと認められた場合はデータの復号化を中止する（ステップ４５１０）。サインの検定に用いるデータセンタ２２００の公開キーは、範囲復号部２０４０にあらかじめ埋め込んでおくか、または外部の認証局から取得するなどの方法で取得する。

【００９９】サインの検定後のデータの部分範囲の復号化処理は、第１の実施の形態における図１１のデータの部分範囲の復号化処理と同様の処理である。

【０１００】まず、コンテンツＩＤに対応する暗号化コンテンツデータ２０９０を取得する（ステップ４５２０）。続いて、暗号化コンテンツデータ２０９０から部分データを取り出す（ステップ４５３０）。一つずつ順番に取り出したフレーム画像に対し、範囲復号キー２２８０の範囲情報３６４０，３６５０の範囲に含まれるかをチェックする（ステップ４５４０）。範囲３６４０，３６５０に含まれるフレーム画像は範囲復号キー２２８０の中の全体復号キー３６３０を用いて復号化する（ステップ４５５０）。範囲３６４０，３６５０に含まれないフレーム画像は破棄する（ステップ４５６０）。かかる処理を映像データを構成する全てのフレーム画像について繰り返す（ステップ４５７０）。ステップ４５５０で復号化された部分データを組み直し、範囲復号化コンテンツデータ２０６０を作成し出力する（ステップ４５８０）。ここまでの処理は、第１の実施の形態における図１１のステップ４２２０～ステップ４２８０と同様の処理である。

【０１０１】以上の処理により、サイン付き範囲復号キー５０００を用いて、範囲復号キーの改竄を防ぐことができる。

【０１０２】第３の実施の形態では暗号化データとして部分単位暗号化データ１２８０の集合として表されるデータを用いた例を説明したが、第２の実施の形態の方式を第２の実施の形態で示した全体を暗号化した暗号化データ１０００に適用することもできる。すなわち、第２の実施形態に対してサインによる検定処理を適用できる。

【０１０３】また第３の実施の形態では、データの改竄を防止する方法として、範囲復号キー本体３６００にサインデータ３６６０を付加し、それを検定することでデータの改竄を防止していたが、範囲復号キー本体３６００をデータセンタ２２００と範囲復号部２０４０とが共有する秘密キーで暗号化する方法を用いても良い。すなわち、共有する秘密キーを用いてデータセンタ２２００で範囲復号キーを暗号化し、同じく共有する秘密キーを用いて範囲復号部２０４０で復号化する。これにより、暗号化した範囲復号キーを改竄すると範囲復号部２０４０で正しく範囲復号キーの復号ができず、暗号化データを復号することができなくなる。また、この方式では範囲復号部２０４０ごとに共有秘密キーを変更することにより、ある特定の範囲復号部２０４０に対してのみ暗号化データの復号化ができる範囲復号キーを作成することができる。

【０１０４】さらに、上述した範囲復号キー本体３６００をデータセンタ２２００と範囲復号部２０４０が共有する秘密キーで暗号化したデータに対し、データセンタ２２００のサインを付加することにより、より堅牢なシステムを構成することができる。すなわち、範囲復号キー本体３６００を暗号化する共有秘密キーが漏洩した場合にも、サインデータ３６６０による検定が行われるため範囲復号キーを捏造することができない。また、逆にデータセンタの秘密キーが漏洩した場合にも、共有秘密キーが分からなければ範囲復号キーを生成することができない。

【０１０５】

【発明の効果】以上述べたように、本発明によれば、暗号化データの部分範囲のみを復号化（全体を復号化し部分範囲のみを利用者に渡す方式も含む）するような復号キーが作成でき、この復号キーを用いて暗号化データの部分範囲のみを復号化することができる。この復号キーと復号化装置により、あらかじめ利用者にデータを配布するようなデータ販売システムにおいても、データの部分範囲のみの販売ができる。従って、利用者にあらかじめ配布された暗号化データに対して、利用者が必要とする部分のみを利用させることができ、またその利用部分に応じた利用料を課金することができる。サイン付き範囲復号キーを用いるようにすれば、範囲復号キーの改竄を防ぐことができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態のデータ復号化方法の概念図である。

【図２】第１の実施形態のデータ復号化方法を用いたコンテンツ販売システムのシステムブロック図である。

【図３】第１の実施形態のデータ復号化方法を用いたコンテンツ販売システムの機能ブロックの関連とデータの流れを示す図である。

【図４】第１の実施形態を映像データに適用した場合におけるデータの暗号化・復号化処理の概念図である。

【図５】復号キー管理テーブルの例を示す図である。

【図６】範囲復号キーのデータ構造を示す図である。

【図７】コンテンツ情報検索テーブルの例を示す図である。

【図８】課金管理テーブルの例を示す図である。

【図９】範囲復号キー取得部における範囲復号キー取得処理のフローチャート図である。

【図１０】範囲復号キー生成部における範囲復号キー生成処理のフローチャート図である。

【図１１】範囲復号部におけるコンテンツデータに対す

る部分範囲の復号化処理のフローチャート図である。

【図１２】本発明の第２の実施の形態のデータ復号方法の概念図である。

【図１３】第２の実施の形態の範囲復号部における部分範囲の復号化処理のフローチャート図である。

【図１４】本発明の第３の実施の形態のサイン付き範囲復号キーによるデータ復号化の概念図である。

【図１５】サイン付き範囲復号キーのデータ構造を示す図である

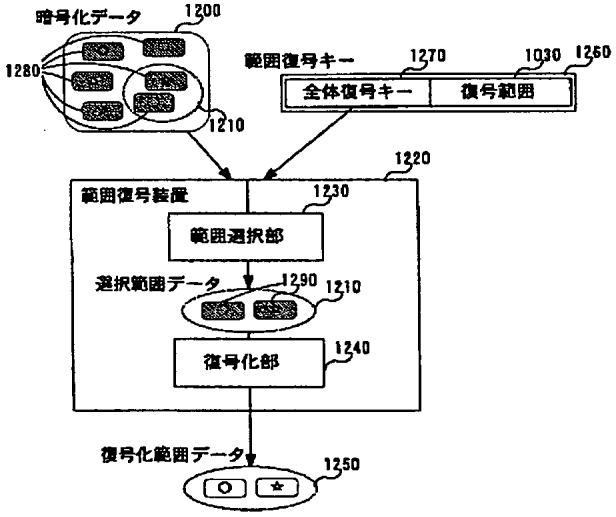
【図１６】サイン付き範囲復号キー生成処理のフローチャート図である。

【図１７】サイン付き範囲復号キーを用いたデータの部分範囲の復号化処理のフローチャート図である。

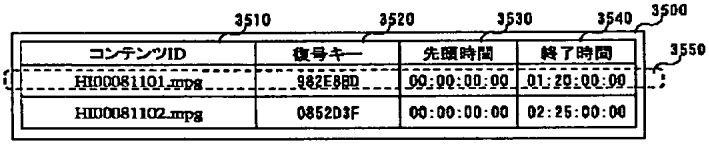
【符号の説明】

１０００……暗号化データ
１２００……集合形式の暗号化データ
１２６０……範囲復号キー
１２７０……全体復号キー
１２６０……復号範囲情報
１２５０……復号化範囲データ
２０３０……コンテンツ利用部分選択部
２０４０……範囲復号部
２０５０……範囲復号キー取得部
２２７０……範囲復号キー生成部
２３００……課金部
５０００……サイン付き範囲復号キー

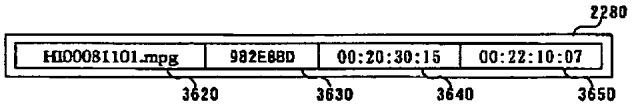
【図１】



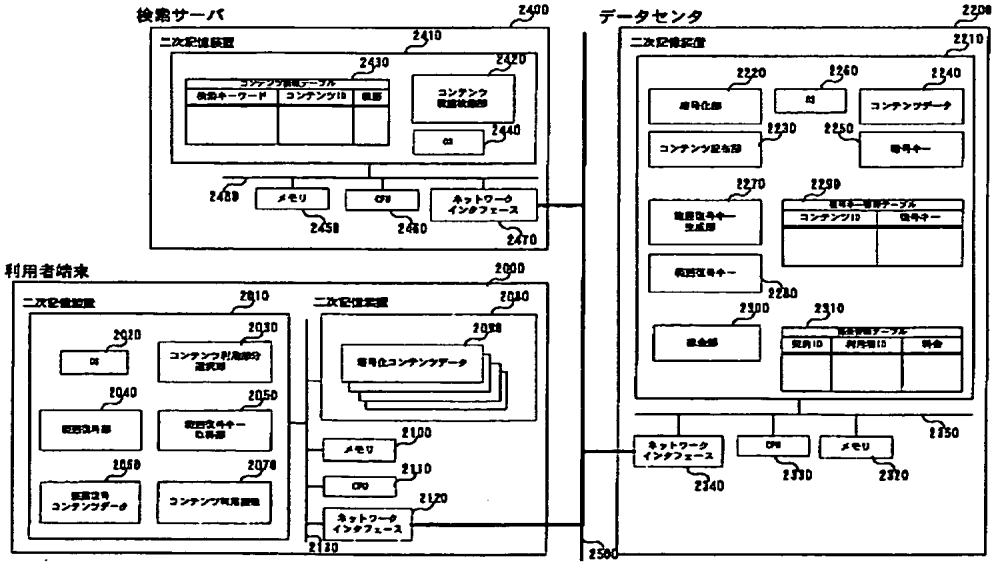
【図５】



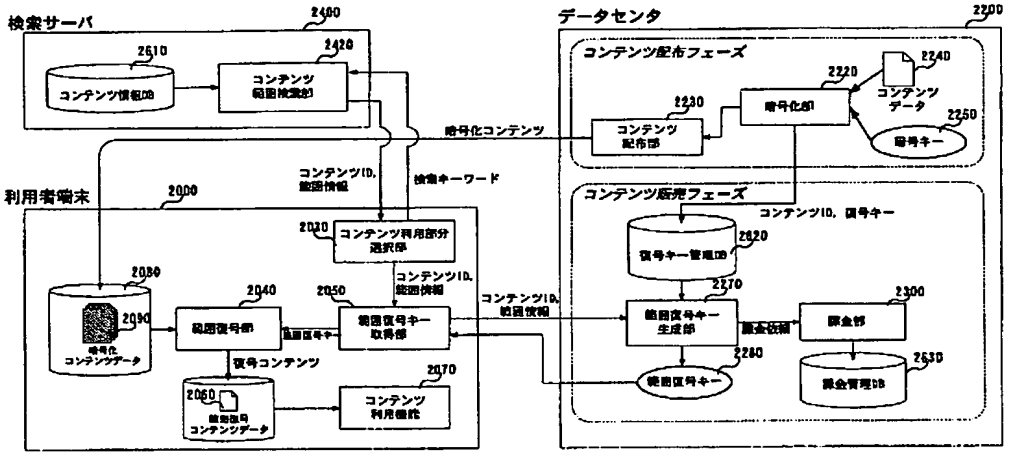
【図６】



【図２】



【図３】



【図７】

3700 映像内容情報	3710 コンテンツID	3720 開始時間	3730 終了時間
春, 青空, 桜の花, 名古屋城	HID0081101.mpg	00:20:30:15	00:22:10:07
夏, 南国, ハイビスカス, 太陽	HID0081102.mpg	00:01:00:00	00:03:29:17

3740 2430

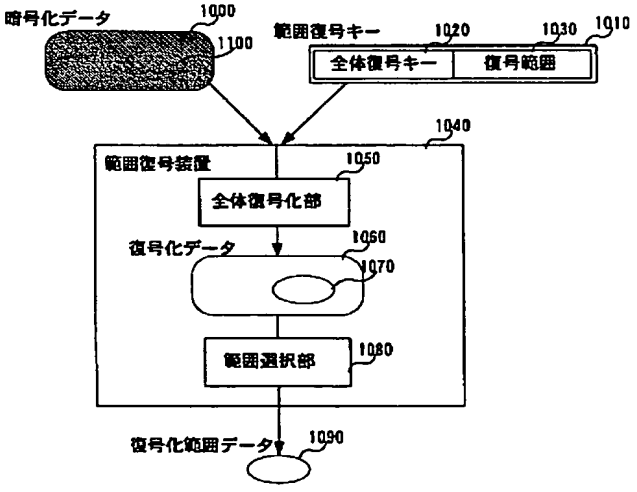
【図８】

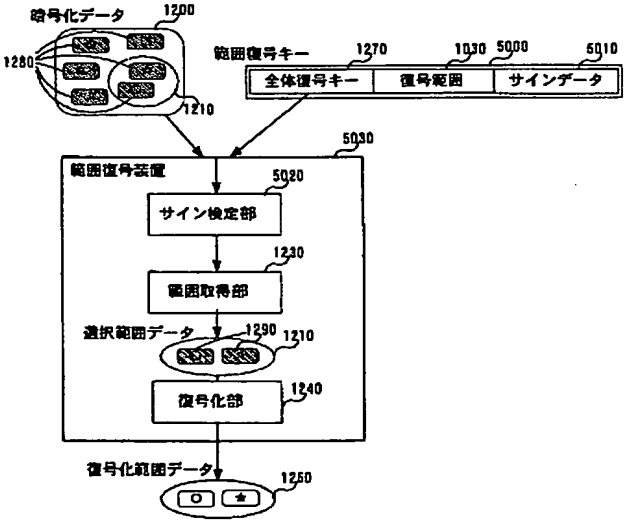
3800 契約ID	3810 利用者ID	3820 料金
208015	MB00001	¥10,000

2310

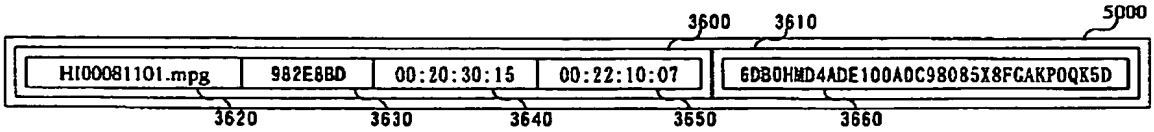
【図１２】

【図１４】

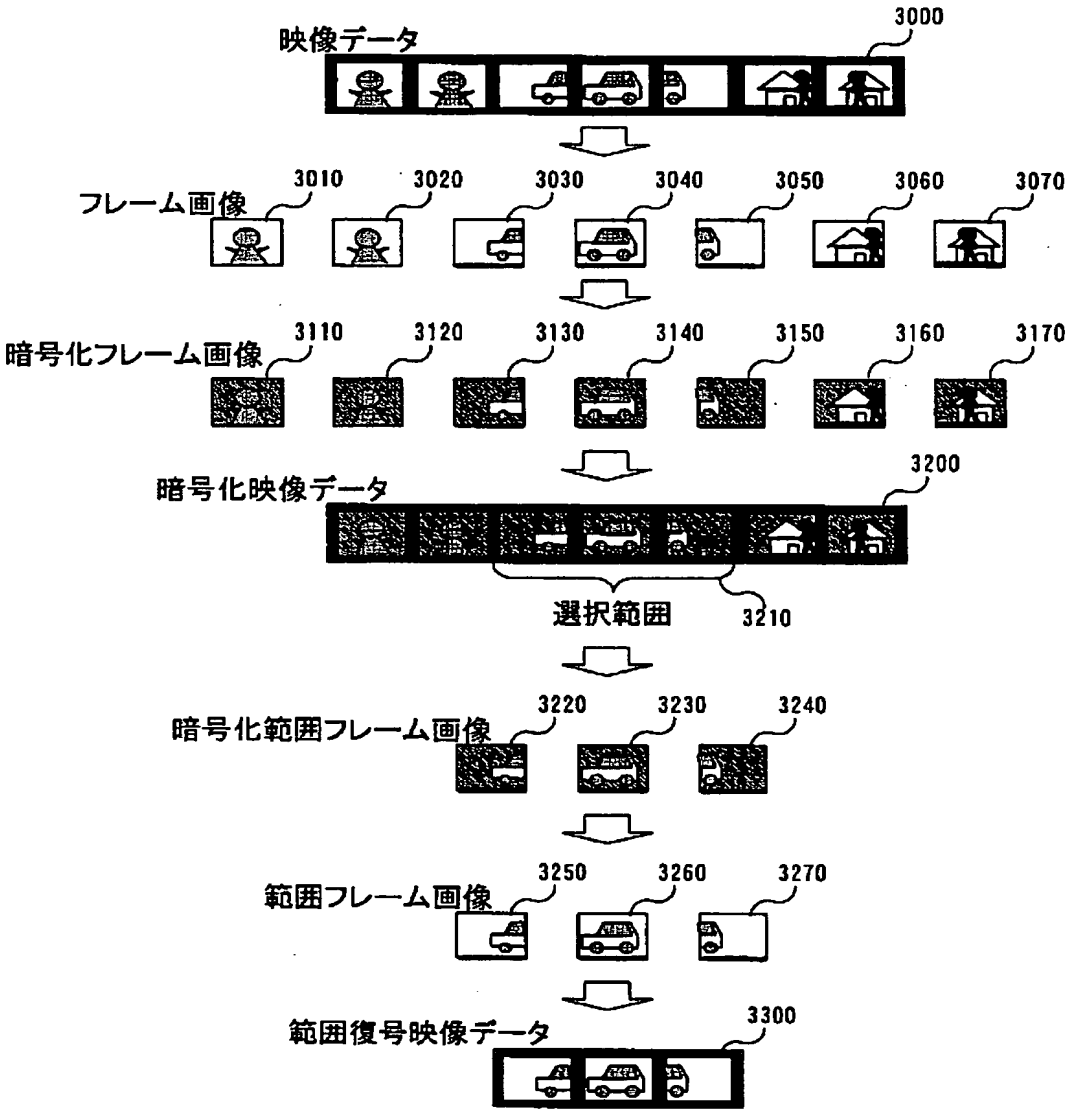




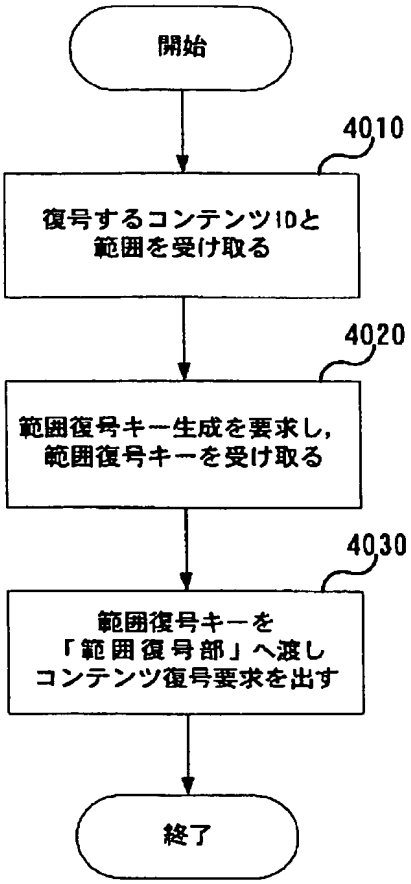
【図１５】



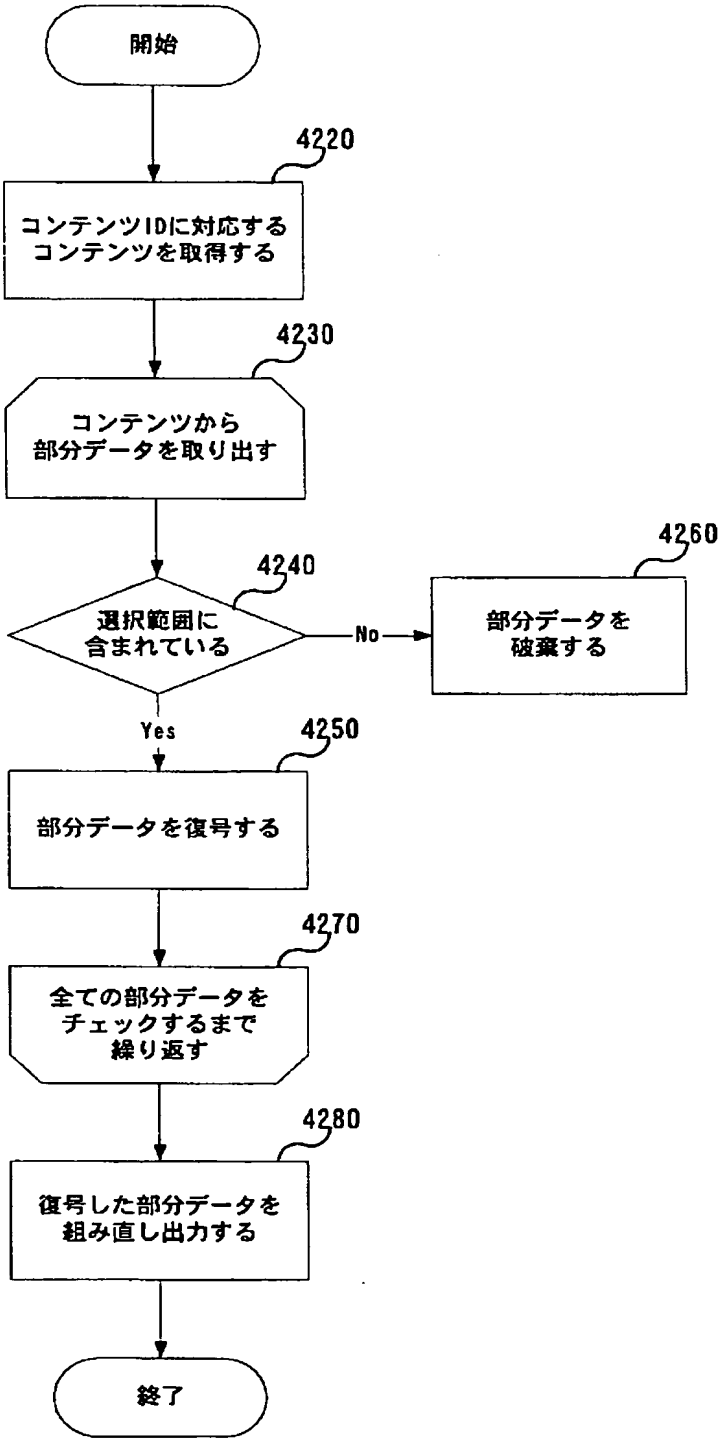
【図４】


映像データ
3000
フレーム画像
3010
3020
3030
3040
3050
3060
3070
暗号化フレーム画像
3110
3120
3130
3140
3150
3160
3170
暗号化映像データ
3200
選択範囲
3210
暗号化範囲フレーム画像
3220
3230
3240
範囲フレーム画像
3250
3260
3270
範囲復号映像データ
3300

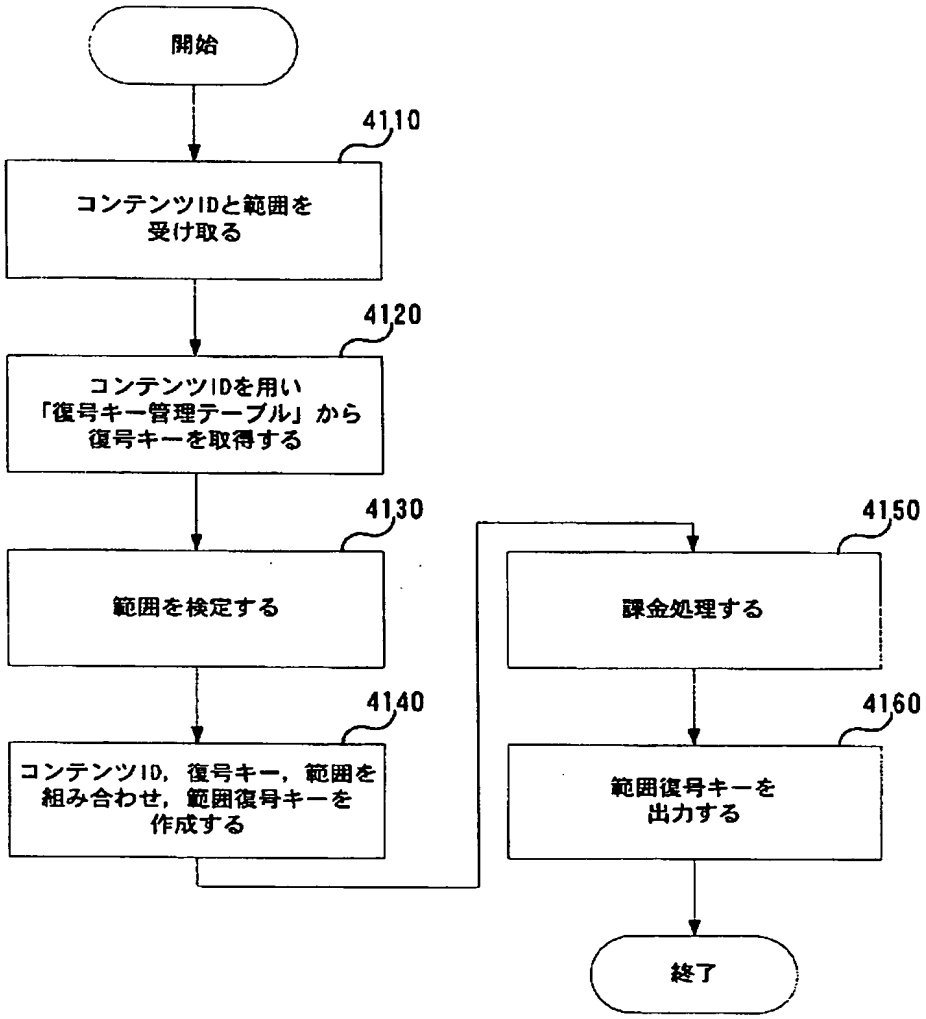
【図９】


開始
4010
復号するコンテンツIDと
範囲を受け取る
4020
範囲復号キー生成を要求し，
範囲復号キーを受け取る
4030
範囲復号キーを
「範囲復号部」へ渡し
コンテンツ復号要求を出す
終了

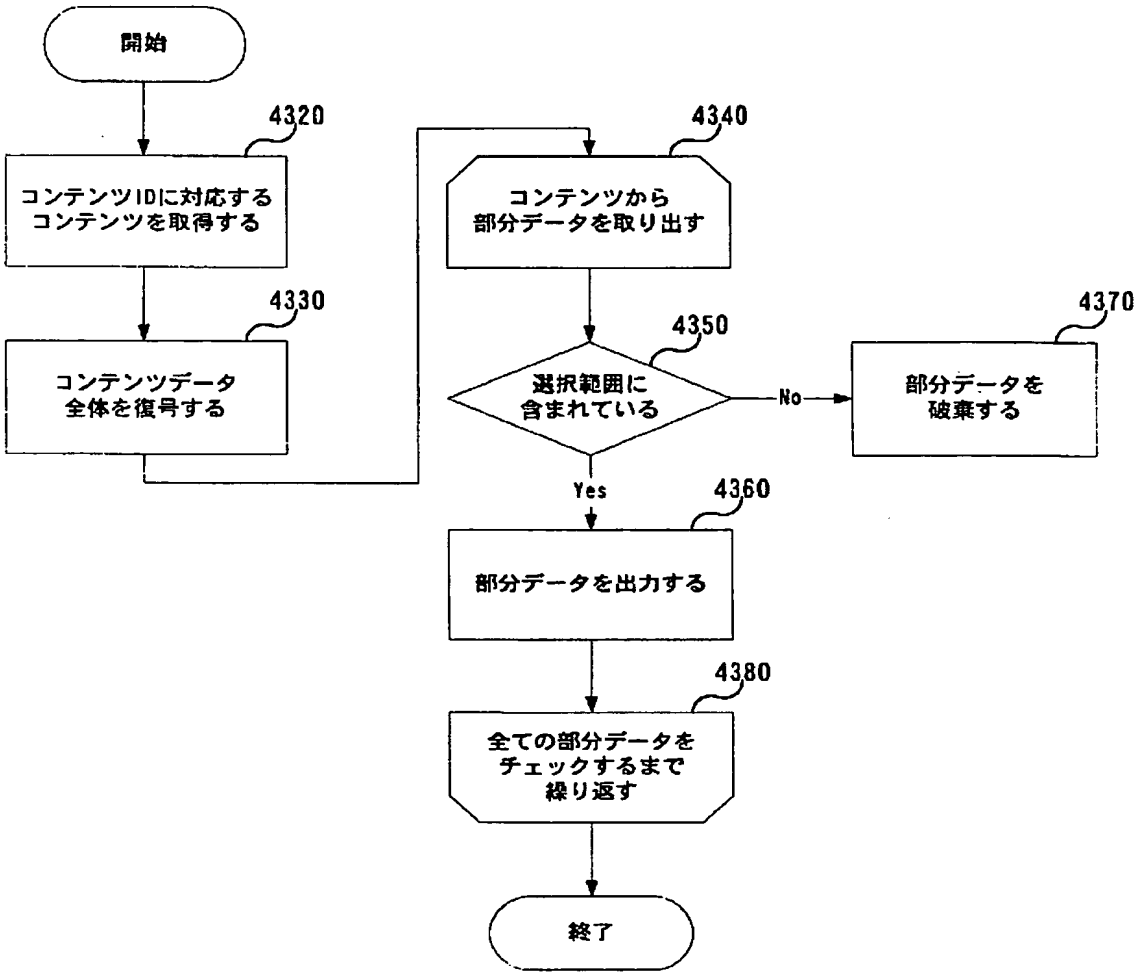
【図１１】


開始
4220
コンテンツIDに対応する
コンテンツを取得する
4230
コンテンツから
部分データを取り出す
4240
選択範囲に
含まれている
No
4260
部分データを
破棄する
Yes
4250
部分データを復号する
4270
全ての部分データを
チェックするまで
繰り返す
4280
復号した部分データを
組み直し出力する
終了

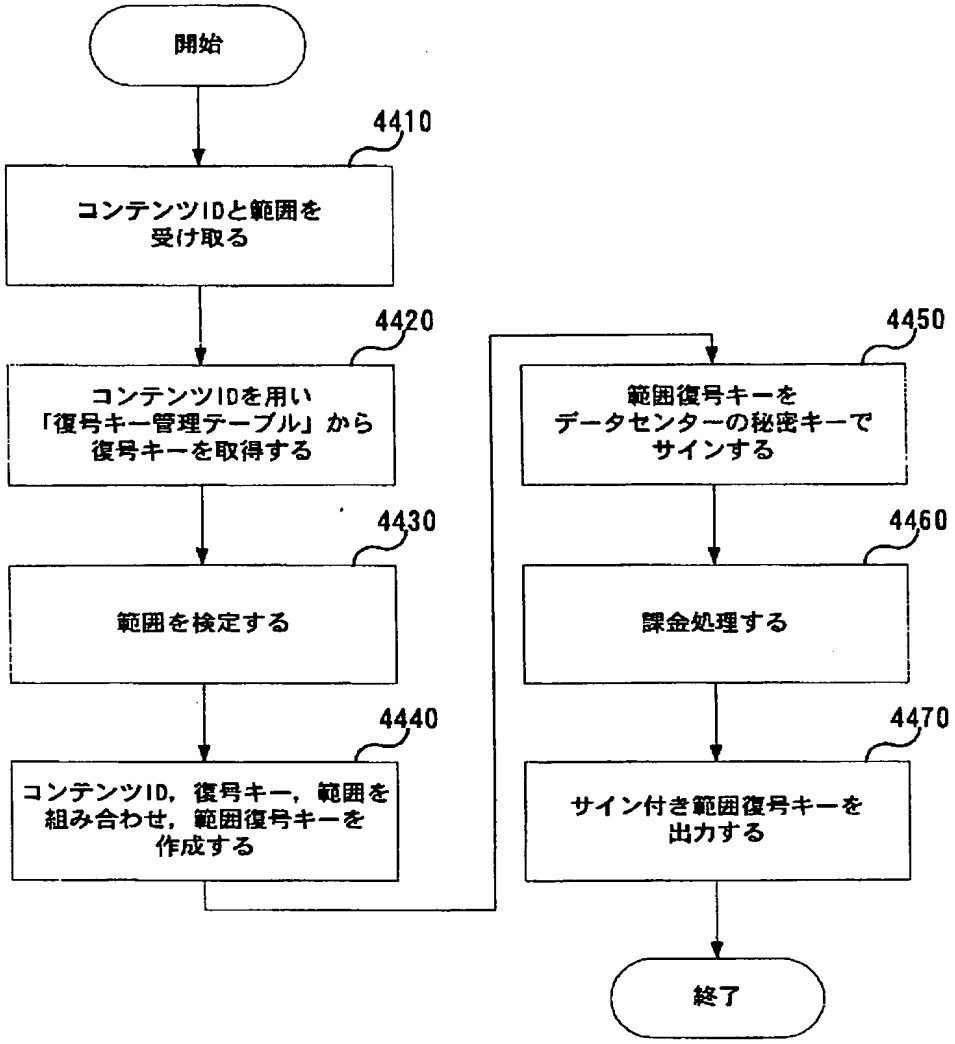
【図１０】


開始
4110
コンテンツIDと範囲を受け取る
4120
コンテンツIDを用い「復号キー管理テーブル」から復号キーを取得する
4130
範囲を検定する
4140
コンテンツID，復号キー，範囲を組み合わせ，範囲復号キーを作成する
4150
課金処理する
4160
範囲復号キーを出力する
終了

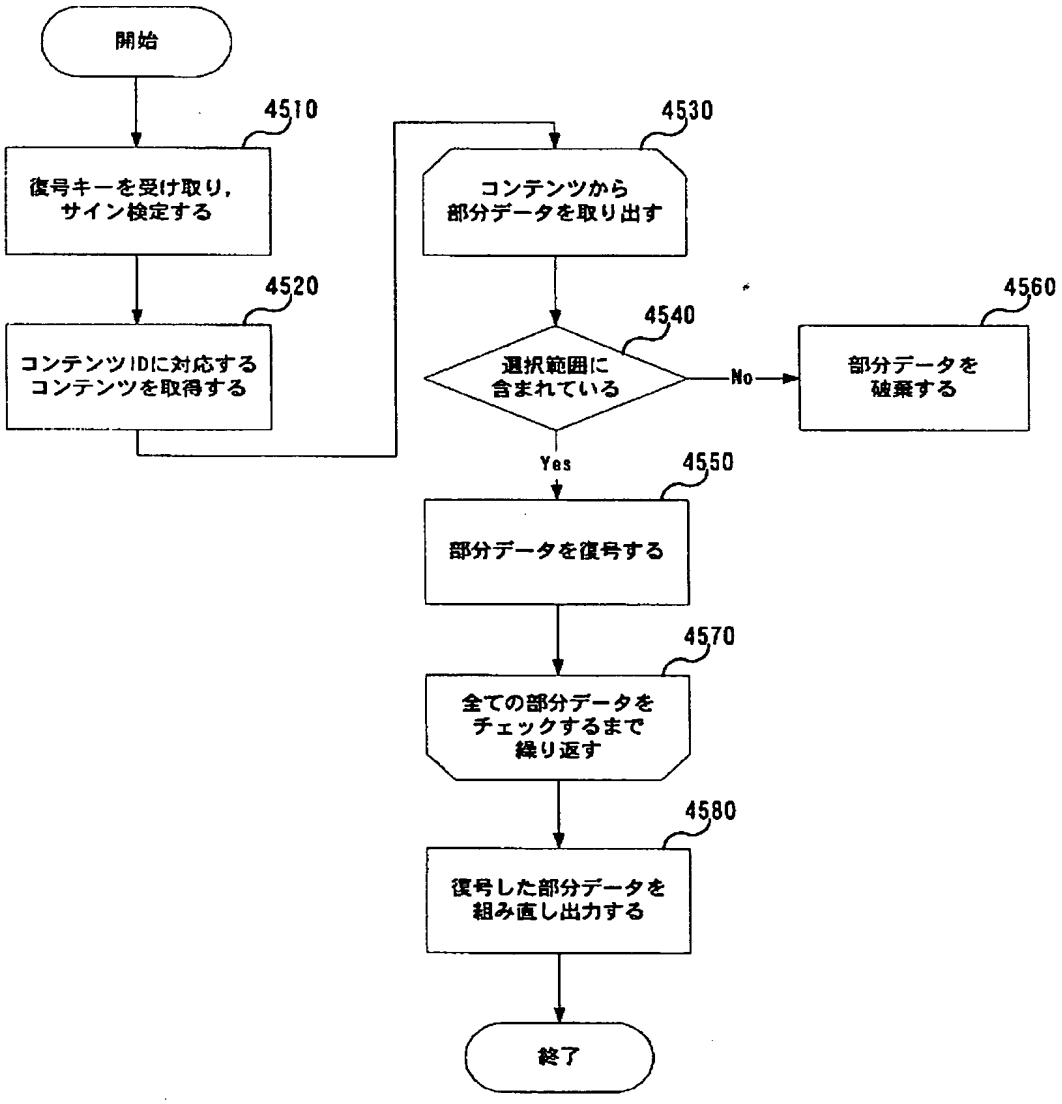
【図１３】


開始
4320
コンテンツIDに対応する
コンテンツを取得する
4330
コンテンツデータ
全体を復号する
4340
コンテンツから
部分データを取り出す
4350
選択範囲に
含まれている
No
4370
部分データを
破棄する
Yes
4360
部分データを出力する
4380
全ての部分データを
チェックするまで
繰り返す
終了

【図１６】


開始
4410
コンテンツIDと範囲を
受け取る
4420
コンテンツIDを用い
「復号キー管理テーブル」から
復号キーを取得する
4430
範囲を検定する
4440
コンテンツID，復号キー，範囲を
組み合わせ，範囲復号キーを
作成する
4450
範囲復号キーを
データセンターの秘密キーで
サインする
4460
課金処理する
4470
サイン付き範囲復号キーを
出力する
終了

【図１７】



フロントページの続き

(72)発明者 岩崎 一正
神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所ビジネスソリューション事業部内
(72)発明者 小林 り恵
神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所ビジネスソリューション事業部内
(72)発明者 小池 博
神奈川県川崎市幸区鹿島田890番地 株式会社日立製作所ビジネスソリューション事業部内
(72)発明者 鳩岡 順一
神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内

Fターム(参考) 5J104 AA01 AA16 EA04 EA15 NA02 PA10